Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

Distribution of the Quaternary Linear Homogeneous Substitutions in a Galois Field into Complete Sets of Conjugate Substitutions.

BY T. M. PUTNAM.

The classification used is based upon the canonical forms of linear homogeneous substitutions in an arbitrary Galois field.*

The homogeneous substitution

$$x' = \alpha_1 x + \alpha_2 y + \alpha_3 z + \alpha_4 w, \quad y' = x, \quad z' = y, \quad w' = z$$

has for its characteristic determinant

$$\Delta(\lambda) \equiv \lambda^4 - \alpha_1 \lambda^3 - \alpha_2 \lambda^2 - \alpha_3 \lambda - \alpha_4 ,$$

where α_1, α_2, α_3, α_4 may be arbitrary marks in the $GF[p^n]$ such that $\alpha_4 \neq 0$. Hence, substitutions exist for which $\Delta(\lambda)$ in the $GF[p^n]$ is irreducible; the product of a linear factor and an irreducible cubic; the product of two distinct irreducible quadratics; the square of an irreducible quadratic; the product of an irreducible quadratic and two linear factors distinct or equal; finally, the product of four linear factors, some or all of which may be equal.

Type I. If the characteristic determinant is irreducible, the substitution may be reduced to the canonical form

$$x' = \lambda x, \quad y' = \lambda^{p^n} y, \quad z' = \lambda^{p^{2n}} z, \quad w' = \lambda^{p^{3n}} w.$$

where λ is an arbitrary mark in the $GF[p^{4n}]$ but not in the $GF[p^{2n}]$. There are then $p^{4n} - p^{2n}$ ways of setting up this canonical form. But replacing λ by λ^{p^n}, $\lambda^{p^{2n}}$, or $\lambda^{p^{3n}}$, we obtain a substitution conjugate with the original. This can

* Dr. L. E. Dickson, Amer. Jour. of Math., vol. XXII, pp. 121–137.

happen by no other replacement; hence, there are $\frac{p^{4n}-p^{2n}}{4}$ distinct sets of conjugate substitutions. The most general substitution commutative with one of this type is

$$x'=\mu x,\quad y'=\mu^{p^n}y,\quad z'=\mu^{p^{2n}}z,\quad w'=\mu^{p^{3n}}w,$$

where μ is an arbitrary mark $\neq 0$ in the $GF[p^{4n}]$. There are then $p^{4n}-1$ substitutions commutative with each one of this type. Hence, each set contains $\frac{N}{p^{4n}-1}$ conjugate substitutions, N being the order of the group, viz., $(p^{4n}-1)(p^{4n}-p^n)(p^{4n}-p^{2n})(p^{4n}-p^{3n})$. The total number of substitutions, then, that can be reduced to this canonical form is $\frac{(p^{4n}-p^{2n})N}{4(p^{4n}-1)}$. The period of any one of them is evidently a factor of $p^{4n}-1$ but not of $p^{2n}-1$.

Type II. If the characteristic determinant is the product of an irreducible cubic and a linear factor, the canonical form becomes

$$x'=\lambda x,\quad y'=\lambda^{p^n}y,\quad z'=\lambda^{p^{2n}}z,\quad w'=\alpha w,$$

where λ is an arbitrary mark in the $GF[p^{3n}]$, but not in the $GF[p^n]$, and α is arbitrary in the $GF[p^n]$. The period of a substitution of this type will be a factor of $p^{3n}-1$, but not of p^n-1. λ can take $p^{3n}-p^n$ values and α can take p^n-1, but replacing λ by $\lambda^{\ n}$ or $\lambda^{p^{2n}}$, we obtain substitutions conjugate with the original. Hence, there are $\frac{(p^{3n}-p^n)(p^n-1)}{3}$ distinct sets of conjugate substitutions. The general substitution commutative with one of this type has the form

$$x'=\mu x,\quad y'=\mu^{p^n}y,\quad z'=\mu^{p^{2n}}z,\quad w'=\beta w,$$

where μ is arbitrary in the $GF\ [p^{3n}]$ and β in the $GF[p^n]$, in all, then, $(p^{3n}-1)(p^n-1)$. Hence, there are $\frac{N}{(p^{3n}-1)(p^n-1)}$ substitutions in each of the conjugate sets, giving in all $\frac{(p^{3n}-p^n)N}{3(p^{3n}-1)}$ substitutions reducible to this canonical form.

Type III. When the characteristic determinant is the product of two distinct quadratics, the canonical form becomes

$$x' = \lambda x, \quad y' = \lambda^p y, \quad z' = \mu z, \quad w' = \mu^p w,$$

where λ and μ are any marks in the $GF[p^{2n}]$ not in the $GF[p^n]$ and $\mu \neq \lambda$ and $\mu \neq \lambda^{p^n}$. There are evidently $(p^{2n} - p^n)(p^{2n} - p^n - 2)$ ways of setting up this canonical form; for to each of the $p^{2n} - p^n$ values of λ, μ takes $p^{2n} - p^n - 2$ values not equal to λ or λ^{p^n}. But the substitutions with the multipliers $(\lambda, \lambda^{p^n}, \mu, \mu^{p^n})$, $(\lambda^{p^n}, \lambda, \mu, \mu^{p^n})$, $(\lambda, \lambda^{p^n}, \mu^{p^n}, \mu)$, $(\lambda^{p^n}, \lambda, \mu^{p^n}, \mu)$ and the four others with the λ's and μ's interchanged are conjugates. Hence, there are $\frac{1}{8}(p^{2n} - p^n)(p^{2n} - p^n - 2)$ distinct sets of conjugate substitutions. The form of the commutative substitution here is

$$x' = \sigma x, \quad y' = \sigma^{p^n} y, \quad z' = v z, \quad w' = v^{p^n} w, \qquad (\sigma,\ v \text{ arb. in } GF[p^{2n}]).$$

The total number of commutative substitutions is then $(p^{2n} - 1)^2$, and hence each set has $\dfrac{N}{(p^{2n}-1)^2}$ substitutions. In all there are, then, $\dfrac{Np^n(p^n - 2)}{8(p^{2n} - 1)}$ substitutions of this type, each of period a factor of $p^{2n} - 1$ but not of $p^n - 1$.

Type IV. The characteristic equation for this type is the square of an irreducible quadratic. Two canonical forms occur,

$$\begin{aligned}
&(1)\quad x' = \lambda x, \quad y' = \lambda(y + x), \quad z' = \lambda^{p^n} z, \quad w' = \lambda^{p^n}(w + z);\\
&(2)\quad x' = \lambda x, \quad y' = \lambda y, \qquad\quad\ \ z' = \lambda^{p^n} z, \quad w' = \lambda^{p^n} w,
\end{aligned}$$

where λ is arbitrary in the $GF[p^{2n}]$, but is not in the $GF[p^n]$. There will be $\dfrac{p^{2n} - p^n}{2}$ distinct sets of conjugate substitutions in each case. The corresponding commutative substitutions are

$$\text{(i)} \quad x' = \mu x, \quad y' = \sigma x + \mu y, \quad z' = \mu^{p^n} z, \quad w' = \sigma^{p^n} z + \mu^{p^n} w,$$

μ and σ being arbitrary in the $GF[p^{2n}]$.

$$\text{(ii)} \quad x' = \sigma_1 x + \mu_1 y, \quad y' = \sigma_2 x + \mu_2 y, \quad z' = \sigma_1^{p^n} z + \mu_1^{p^n} w, \quad w' = \sigma_2^{p^n} z + \mu_2^{p^n} w,$$

where σ_1, σ_2, μ_1, μ_2 are arbitrary marks of the $GF[p^{2n}]$. There are $p^{2n}(p^{2n} - 1)$ of form (i) and $(p^{4n} - 1)(p^{4n} - p^{2n})$ of form (ii), the latter being the number of ways that the determinant of the substitution (ii), viz., $(\sigma_1 \mu_2 - \mu_1 \sigma_2)^{p^n + 1}$ can be set up with $\sigma_1, \sigma_2, \mu_1, \mu_2$ arbitrary marks in the $GF[p^{2n}]$. Hence, from (1) there are in all $\frac{N}{2p^n(p^n+1)}$, and from (2) $\frac{N}{2p^n(p^n+1)(p^{4n}-1)}$ substitutions, those of (1) being of period a factor of $p\,(p^{2n}-1)$ but not of $p\,(p^n-1)$, and those of (2) of period a factor of $p^{2n}-1$ but not of p^n-1.

Type V. When $\Delta(\lambda)$ is the product of an irreducible quadratic and two distinct linear factors, the canonical form is

$$x' = \alpha x, \quad y' = \beta y, \quad z' = \lambda z, \quad w' = \lambda^{p^n} w,$$

where α and β are arbitrary in the $GF[p^n]$, $\alpha \neq \beta$, and λ is arbitrary in the $GF[p^{2n}]$ but not in the $GF[p^n]$. If α and β, or λ and λ^{p^n} are interchanged, conjugate substitutions are obtained; hence, there are $\frac{(p^{2n}-p^n)(p^n-1)(p^n-2)}{4}$ distinct sets of conjugate substitutions. The commutative substitutions are of the form

$$x' = ax, \quad y' = by, \quad z' = \mu z, \quad w' = \mu^{p^n} w,$$

with a and b arbitrary in the $GF[p^n]$, and μ arbitrary in the $GF[p^{2n}]$, in all, therefore, $(p^{2n}-1)(p^n-1)^2$. Hence there are from this type $\frac{p^n(p^n-2)N}{4(p^{2n}-1)}$ substitutions of period a factor of $p^{2n}-1$ but not of p^n-1.

Type VI. $\Delta(\lambda)$ for this type is the same as in Type V with the two linear factors coincident. Two canonical forms occur,

$$(1)\quad x' = \alpha x, \quad y' = \alpha(y+x), \quad z' = \lambda z, \quad w' = \lambda^p w;$$
$$(2)\quad x' = \alpha x, \quad y' = \alpha y, \quad z' = \lambda z, \quad w' = \lambda^{p^n} w.$$

(1) is of period a factor of $p\,(p^{2n}-1)$ but not of $p\,(p^n-1)$, and (2) is of period a factor of $(p^{2n}-1)$ but not of p^n-1. In each case there are $\frac{(p^{2n}-p^n)(p^n-1)}{2}$ distinct sets of conjugate substitutions. The commutative substitutions have the respective forms,

$$\text{(i)}\quad x' = ax, \quad y' = by + ax, \quad z' = \mu z, \quad w' = \mu^{p^n} w;$$
$$\text{(ii)}\quad x' = ax + by, \quad y' = cx + dy, \quad z' = \mu z, \quad w' = \mu^{p^n} w.$$

There are $p^n(p^n-1)(p^{2n}-1)$ of form (i) and $(p^{2n}-1)^2(p^{2n}-p^n)$ of form (ii).

Hence, belonging to the two canonical forms, there are respectively $\frac{N}{2(p^n+1)}$ and $\frac{N}{2(p^n+1)(p^{2n}-1)}$ substitutions.

Type VII. In this case $\Delta(\lambda)$ is the product of four distinct linear factors. The canonical form is

$$x' = \alpha x, \quad y' = \beta y, \quad z' = \gamma z, \quad w' = \delta w.$$

The determinant of this substitution is $\Delta = \alpha\beta\gamma\delta$, with $(p^n-1)^4$ sets of solutions. But three multipliers are equal in $4(p^n-1)(p^n-2)$ of the sets [see IX]; two only will be equal for $6(p^n-1)(p^n-2)(p^n-3)$ others [see VIII]; they will be equal in pairs in $3(p^n-1)(p^n-2)$ of the sets [XI], while for p^n-1 all four will be equal [X]. Excluding these, there remain $(p^n-1)(p^n-2)(p^n-3)(p^n-4)$ sets of distinct multipliers conjugate, however, in sets of 4!. A substitution of this type is commutative with the $(p^n-1)^4$ substitutions of the form

$$x' = ax, \quad y' = by, \quad z' = cz, \quad w' = dw.$$

Hence there are $\frac{1}{24}(p^n-1)(p^n-2)(p^n-3)(p^n-4)$ sets with $\frac{N}{(p^n-1)^4}$ substitutions in each; in all, therefore, there are $\frac{(p^n-2)(p^n-3)(p^n-4)N}{24(p^n-1)^3}$ substitutions of period a factor of p^n-1 from this type.

Type VIII. For this type just two of the linear factors of $\Delta(\lambda)$ are equal, the canonical forms being

$$\begin{aligned}&(1)\quad x' = \alpha x, \quad y' = \beta y, \quad z' = \gamma z, \quad w' = \gamma(w+z);\\ &(2)\quad x' = \alpha x, \quad y' = \beta y, \quad z' = \gamma z, \quad w' = \gamma w,\end{aligned}$$

(1) is of period a factor of $p(p^n-1)$ and (2) is of period a factor of p^n-1. For each there are $\frac{(p^n-1)(p^n-2)(p^n-3)}{2}$ distinct sets of conjugate substitutions. The $p^n(p_n-1)^3$ substitutions of the form

$$x' = ax, \quad y' = by, \quad z' = cz, \quad w' = dz + cw$$

are commutative with (1), while there are $(p^n - 1)^2 (p^{2n} - 1)(p^{2n} - p^n)$ commutative with (2), viz., all those of the form

$$x' = ax, \quad y' = by, \quad z' = cz + dw, \quad w' = c'z + d'w.$$

Therefore, there are $\frac{(p^n - 2)(p^n - 3) N}{2p^n (p^n - 1)^2}$ substitutions of type (1) and $\frac{(p^n - 2)(p^n - 3) N}{2 (p^n - 1)^3 (p^n + 1) p^n}$ of type (2).

Type IX. In this case there are three of the linear factors of $\Delta(\lambda)$ equal, giving rise to three canonical forms,

$$\begin{array}{llll}
(1) & x' = \alpha x, & y' = \beta y, & z' = \beta (z + y), & w' = \beta (w + z), \\
(2) & x' = \alpha x, & y' = \beta y, & z' = \beta z, & w' = \beta (w + z), \\
(3) & x' = \alpha x, & y' = \beta y, & z' = \beta z, & w' = \beta w.
\end{array}$$

(1) and (2) are of periods factors of $p(p^n - 1)$ (if $p = 2$, (1) is of period a factor of $4(p^n - 1)$), (3) is of period a factor of $p^n - 1$. There are just $(p^n - 1)(p^n - 2)$ sets of conjugate substitutions for each subtype.

The respective substitutions commutative with (1), (2) and (3) have the forms

$$\begin{array}{lllll}
\text{(i)} & x' = ax, & y' = by, & z' = bz + cy, & w' = bw + cz + dy; \\
\text{(ii)} & x' = ax, & y' = by + cz, & z' = dz, & w' = ey + fz + dw; \\
\text{(iii)} & x' = dx, & y' = a_1 y + b_1 z + c_1 w, & z' = a_2 y + b_2 z + c_2 w, & \\
& & & & w' = a_3 y + b_3 z + c_3 w.
\end{array}$$

There are $p^{2n} (p^n - 1)^2$ of form (i), $p^{3n} (p^n - 1)^3$ of form (ii), and $(p^{3n} - 1)(p^{3n} - p^n)(p^{3n} - p^{2n})(p^n - 1)$ of form (iii). There will be then in all $\frac{(p^n - 2) N}{p^{2n} (p^n - 1)}$ substitutions from the subtype (1), $\frac{(p^n - 2) N}{p^{3n}(p^n - 1)^2}$ from (2), and $\frac{(p^n - 2) N}{(p^{3n} - 1)(p^{3n} - p^n)(p^{3n} - p^{2n})}$ from (3).

Type X. When $\Delta(\lambda)$ is the fourth power of a single linear factor, five canonical forms arise,

$$\begin{array}{lllll}
(1) & x' = \alpha x, & y' = \alpha (y + x), & z' = \alpha (z + y), & w' = \alpha (w + z); \\
(2) & x' = \alpha x, & y' = \alpha y, & z' = \alpha (z + y), & w' = \alpha (w + z); \\
(3) & x' = \alpha x, & y' = \alpha (y + x), & z' = \alpha z, & w' = \alpha (w + z); \\
(4) & x' = \alpha x, & y' = \alpha y, & z' = \alpha z, & w' = \alpha (w + z); \\
(5) & x' = \alpha x, & y' = \alpha y, & z' = \alpha z, & w' = \alpha w.
\end{array}$$

If $p = 2$, (1) and (2) are of period $4\,(p^n - 1)$ or a factor of it; if $p = 3$, (1) is of period a factor of $9\,(p^n - 1)$; for $p > 3$, the period of (1) is a factor of $p\,(p^n - 1)$; for $p > 2$, the period of (2) is a factor of $p\,(p^n - 1)$. (3) and (4) are always of period a factor of $p\,(p^n - 1)$, and (5) is of period a factor of $p^n - 1$.

The substitutions commutative with the above have the respective forms

(i) $x' = ax, \quad y' = bx + ay, \quad z' = cx + by + az,$
$w' = dx + cy + bz + aw;$

(ii) $x' = ax + by, \quad y' = cy, \quad z' = dy + cz,$
$w' = ex + fy + dz + cw;$

(iii) $x' = a_1 x + b_1 y, \quad y' = a_2 x + a_1 y + b_2 z + b_1 w, \quad z' = a_3 x + b_3 z,$
$w' = a_4 x + a_3 y + b_4 z + b_3 w;$

(iv) $x' = ax + by + cz, \quad y' = a_1 x + b_1 y + c_1 z, \quad z' = c_2 z,$
$w' = a_4 x + b_4 y + c_4 z + c_2 w;$

(v) is commutative with every substitution of the group.

The number of substitutions in each of these types is

(1) $p^{3n}(p^n - 1)$, (2) $p^{4n}(p^n - 1)^2$,
(3) $p^{4n}(p^{2n} - 1)(p^{2n} - p^n)$, (4) $p^{5n}(p^n - 1)(p^{2n} - 1)(p^{2n} - p^n)$.

Hence the totals for the respective subtypes are

$$(1)\ \frac{N}{p^{3n}}, \quad (2)\ \frac{N}{p^{4n}(p^n - 1)}, \quad (3)\ \frac{N}{p^{5n}(p^{2n} - 1)}, \quad (4)\ \frac{N}{p^{6n}(p^{2n} - 1)(p^n - 1)},$$

and, finally (5) with $p^n - 1$ substitutions.

Type XI. When the multipliers are equal in pairs, three canonical forms arise,

(1) $x' = \alpha x, \quad y' = \alpha(y + x), \quad z' = \beta z, \quad w' = \beta(w + z);$
(2) $x' = \alpha x, \quad y' = \alpha y, \quad z' = \beta z, \quad w' = \beta(w + z);$
(3) $x' = \alpha x, \quad y' = \alpha y, \quad z' = \beta z, \quad w' = \beta w.$

There will be $\dfrac{(p^n - 1)(p^n - 2)}{2}$ distinct sets of conjugate substitutions for (1) and (3), since interchanging α and β gives conjugate substitutions. This is not true, however, for (2), which has, therefore, $(p^n - 1)(p^n - 2)$ distinct sets.

The substitutions commutative with these three subtypes are, respectively,

$$\begin{array}{lllll}
\text{(i)} & x' = ax, & y' = bx + ay, & z' = cz, & w' = dz + cw\,; \\
\text{(ii)} & x' = ax + by, & y' = cx + dy, & z' = ez, & w' = fz + ew, \\
\text{(iii)} & x' = ax + by, & y' = a_1x + b_1y, & z' = cz + dw, & w' = c_1z + d_1w.
\end{array}$$

There will be $p^{2n}(p^n - 1)^2$ substitutions of form (i), $p^{2n}(p^n - 1)^3(p^n + 1)$ of form (ii), and $(p^{2n} - 1)^2(p^{2n} - p^n)^2$ of form (iii). The total number of substitutions of each type is, therefore,

$$(1)\ \frac{(p^n - 2)\,N}{2\,(p^n - 1)\,p^{2n}}, \quad (2)\ \frac{(p^n - 2)\,N}{p^{2n}\,(p^n - 1)^2(p^n + 1)}, \quad (3)\ \frac{(p^n - 2)\,N}{2\,(p^{2n} - p^n)^2(p^n + 1)\,(p^{2n} - 1)}.$$

As a check on the above results, the sum of all the totals for the various canonical forms will be found to equal N, the order of the group. For $p^n = 2$ the group is simply isomorphic with the alternating group on eight letters, and the above results also agree with those for that group.

UNIVERSITY OF TEXAS, *May*, 1900.